



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,381	09/30/2003	Rahul Khanna	42.P17236	6856
7590	11/17/2006		EXAMINER	
R. Alan Burnett BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP Seventh Floor 12400 Wilshire Boulevard Los Angeles, CA 90025-1026			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2135	
DATE MAILED: 11/17/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/675,381	KHANNA ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 30 September 2003.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-30 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

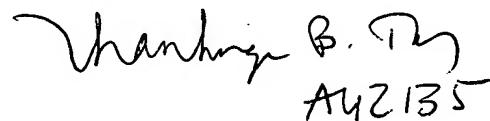
Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 30 September 2003 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.



 AY2135

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application
- 6) Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on September 30, 2003. Claims 1-30 are pending. At this time, claims 1-30 are rejected.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 23-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

a. Referring to claim 23:

(1) Claim 23 recites a machine-readable media providing instructions to perform operations on a computer system. It does contain a useful method and would normally be considered statutory. However, the applicant's specification defines "a machine-readable medium can include propagated signals such as electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.) (see page 21, lines 1-2 of applicant's specification)", wherein these intangible media such as signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived absent the tangible medium through which they are conveyed. Thus, claim 23 does not recite any structure, i.e., machine to carry out the functions of all the recited steps. Therefore, claim 23 recites non-statutory subject matter. Claims 24-30 depend on claim 23, therefore they are rejected with the same rationale applied against claim 23 above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-3, 8-11, 15-19, and 23-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cox et al (US 5,349,643), and further in view of Zimmer et al (US 2004/0193867 A1).

a. Referring to claim 1:

i. Cox teaches:

(1) authenticating, during a pre-boot phase of a client (**column 3, lines 58-64 of Cox**), a boot server on which an operating system (OS) boot image is stored (**column 3, lines 15-27 of Cox**);

(2) downloading an OS boot image from the boot server if it is authenticated (**column 3, lines 24-27 of Cox**); and

(3) loading the OS boot image on the client (**column 3, lines 24-27 of Cox**).

ii. Although Cox implies the authentication during pre-boot phase in column 3, lines 58-64, Cox is silent on the capability of using PXE for the pre-boot phase. On the other hand, Zimmer teaches the PXE as shown in paragraph 0017 of Zimmer.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Cox with the teachings of Zimmer (if indeed is not inherent in Cox's boot server) for enhancing the security of these networks (**column 1, lines 53-54 of Cox**).

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Cox with the teachings of Zimmer to provide an improved boot architecture (**column 2, lines 44-45 of Cox**).

b. Referring to claim 2:

i. Cox further teaches:

(1) wherein the boot server is authenticated by comparing a shared secret stored by the client with a corresponding shared secret stored by the boot server (**column 6, lines 29-40 and column 8, lines 25-31 of Cox**).

Art Unit: 2135

c. Referring to claim 3:

i. Cox further teaches:

(1) further comprising provisioning the shared secret to at least one of the client and the boot server during a one-time provisioning event such that both the client and the boot server have access to the shared secret (**column 8, lines 25-31 of Cox**).

d. Referring to claims 8 and 10:

i. The combination of teaching between Cox and Zimmer teaches the claimed subject matter and Zimmer further teaches:

(1) wherein the boot server and the client are authenticated using an authenticated dynamic host configuration protocol (DHCP) message exchange process (**paragraphs 0005-0006 of Zimmer**).

e. Referring to claim 9:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

f. Referring to claim 11:

i. Cox further teaches:

(1) wherein the boot server is authenticated by performing the operations of: encrypting the shared secret stored at the client (**column 6, lines 34-40 and column 7, lines 5-8 of Cox**); passing the encrypted shared secret to one of the boot server and an authentication proxy for the boot server (**column 6, lines 34-40 and column 7, lines 5-41 of Cox**); decrypting the encrypted shared secret at said one of the boot server and the proxy for the boot server (**column 6, lines 34-40 and column 7, lines 29-41 of Cox**); and comparing (e.g., verifying) a shared secret stored at said one of the boot server and the authentication proxy for the boot server with the encrypted shared secret that is decrypted (**column 7, lines 29-41 of Cox**).

g. Referring to claim 15:

i. This claim consist a computer system to implement claim 1 and thus it is rejected with the same rationale applied against claim 1 above.

ii. Cox further teaches:

(1) a processor (**column 7, line 2 of Cox**);
(2) memory, coupled to the processor (**column 7, line 2 of Cox**);

(3) a network interface, coupled to the processor; a firmware storage device, coupled to the processor; having firmware instructions stored therein that when executed on the processor cause operations to be performed (**Figure 2 of Cox and column 4, lines 23-60 of Cox**).

h. Referring to claim 16:

i. Cox further teaches:

(1) wherein the boot server is authenticated by comparing a shared secret stored by the computer system with a corresponding shared secret stored by the boot server (**column 7, lines 29-41 of Cox**).

i. Referring to claims 17-18, 28-29:

i. These claims have limitations that is similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

j. Referring to claim 19:

i. This claim has limitations that is similar to those of claims 1 and 11, thus it is rejected with the same rationale applied against claims 1 and 11 above.

k. Referring to claim 23:

i. This claim consist a machine-readable media providing instructions to perform operations on a computer system cited on claim 15 to implement claim 1 and thus it is rejected with the same rationale applied against claims 1, and 15 above.

l. Referring to claim 24:

i. Cox further teaches:

(1) wherein the media comprises a firmware storage device (e.g., memory) and the instructions comprise firmware instructions (**column 7, line 2 of Cox**).

m. Referring to claim 25:

Art Unit: 2135

i. Cox further teaches:

(1) wherein execution of the instructions performs the further operation of broadcasting a boot server discovery message to locate the boot server (**column 4, lines 48-51 of Cox**).

n. Referring to claim 26:

i. This claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

o. Referring to claim 27:

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

6. Claims 4-7, 12-14, 20-22, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cox et al (US 5,349,643), and further in view of Zick et al (US 2005/0010680).

a. Referring to claim 4:

i. Cox and Zimmer teach the claimed subject matter and the handshake between the client and the server as shown in Figures 1 and 2 and the shared secret as shown in column 8, lines 25-31; however, they are silent on the capability of using an Extensible Authentication Protocol (EAP message) exchange between an authenticator EAP server and the client. On the other hand, Zick teaches the use of Extensible Authentication Protocol (EAP message) in paragraphs 0010 and 0069 of Zick.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the modified-invention of Cox with the teachings of Zick (if indeed is not inherent in Cox's system) for enhancing the security of these networks (**column 1, lines 53-54 of Cox**).

iv. The ordinary skilled person would have been motivated to:

(1) have modified the modified-invention of Cox with the teachings of Zick for securing network registration processes that allow two network devices to register with each other, and more particularly to a registration process

Art Unit: 2135

where two devices learn each other's identities and establish a shared key that can later be used by the devices to mutually authenticate each other and to generate session encryption keys (**paragraph 0002 of Zick**).

b. Referring to claim 5:

i. The combination of teaching between Cox, Zimmer, and Zick teaches the claimed subject matter and Zick further teaches:

(1) wherein the shared secret is provisioned from the client to the server and is formulated via a key that is generated by a trusted platform module stored by the client

c. Referring to claim 6:

i. The combination of teaching between Cox, Zimmer, and Zick teaches the claimed subject matter and Zick further teaches:

(1) wherein the shared secret is provisioned using a take ownership protocol under which one of a user or administrator takes ownership of a computer system by providing authentication credentials for that system (**paragraphs 0011, 0038-0039 of Zick**).

d. Referring to claim 7:

i. The combination of teaching between Cox, Zimmer, and Zick teaches the claimed subject matter and Zick further teaches:

(1) wherein the take ownership protocol comprises provisioning authentication credentials via one of the following: provisioning authentication credentials on the client via an out-of-band channel, enabling a user to enter authentication credentials via a local console, and imprinting the client with authentication credentials via remote entry of the authentication credentials by a system administrator (**paragraph 0041 of Zick**).

e. Referring to claim 12:

i. The combination of teaching between Cox, Zimmer, and Zick teaches the claimed subject matter and Zick further teaches:

(1) further comprising: generating a session key; and employing the session key for encryption and decryption of data transferred between the boot server and the client (**paragraph 0109 of Zick**).

f. Referring to claim 13:

i. This claim has limitations that is similar to those of claims 1 and 12, thus it is rejected with the same rationale applied against claims 1 and 12 above.

g. Referring to claim 14:

i. The combination of teaching between Cox, Zimmer, and Zick teaches the claimed subject matter and Zick further teaches:

(1) wherein the shared secret is derived from the combination of a user login and a password corresponding to the user login (**paragraph 0024 of Zick**).

h. Referring to claim 20:

i. This claim has limitations that is similar to those of claims 1 and 12, thus it is rejected with the same rationale applied against claims 1 and 12 above.

i. Referring to claim 21-22:

i. These claims have limitations that is similar to those of claims 5 and 6, thus they are rejected with the same rationale applied against claims 5 and 6 above.

j. Referring to claim 30:

i. The combination of teaching between Cox, Zimmer, and Zick teaches the claimed subject matter; and Cox and Zick further teaches:

(1) wherein execution of the instructions further performs the operations of: generating a user interface on the computer system via which a user can enter authentication credentials (**column 2, lines 17-30 of Cox**); generating a shared secret based on the authentication credentials (**paragraph 0109 of Zick**); and sending the shared secret to the boot server or authentication server (**column 6, lines 34-40 and column 7, lines 5-41 of Cox**).

Art Unit: 2135

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Birse et al (US 7,089300 B1) discloses a method and apparatus are provided for supplying a reliable and maintainable operating system in a net-booted environment. According to one embodiment, a network computer (NC) system including an NC server and multiple NC clients is managed by an NC client causing the remainder of the NC clients that are subsequently booted to receive operating system software that is configured differently than that currently in effect by replacing one or more system volumes on the NC server containing the operating system software with one or more different system volumes (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

November 3, 2006

Thanhnga B. Truong
AU2135